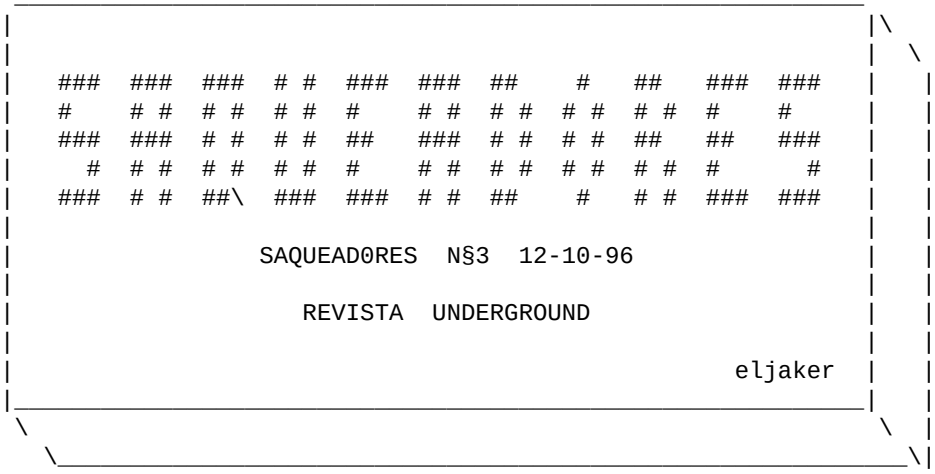

Saqueadores: Revista dedicada al hackin, crackin, virus y demas temas, poco tratados, pero muy interesantes.

Editor: eljaker

Colaboradores: red, warezzman y "el duque de sicilia"

-->Si tienes algo interesante que contar, si quieres ser colaborador o articulista, no dudes en contactar con nosotros.

0. CONTENIDOS:

EOF

1. PRESENTACION:

Parece mentira, pero hemos llegado al tercer numero, y ademas ya tenemos ayuda. Todavia soy el unico articulista, pero pronto llegaran colaboraciones y articulos, de mas gente, para hacer un poco mas variada la revista.

Si tienes algun articulo interesante, sobre estos temas, y te gustaria publicarlo, contacta con nosotros y hazte colaborador, es gratis y recibiras la revista, nada mas salir.

Bueno, el rollo de siempre: Esta revista esta escrita solo con fines educativos, sus autores no se responsabilizan del uso que se pueda hacer con su informacion. Puede ser libremente distribuida y modificada, siempre que se mencionen a sus autores originales.

Vamos al grano....

eljaker

EOF

2. Haciendo una lista de ataque

$Que es --> Una lista de ataque es una recopilacion de los passwords mas habituales o los mas probables.

$Para que sirve --> Sirve, para hackear un ordenador en el que no tienes una cuenta, pero conoces algun login, y necesitas su password. La lista de ataque contiene los passwords mas probables para esa cuenta.

$Como se usa --> Se puede usar:
-A mano, introduciendo tu mismo, los passwords cuando te los pida, esto es un poco pesado y lento, por lo que la lista tiene que ser corta y muy especifica.
-Los puede usar un programa de asalto, programa que hace el login automaticamente, esto solo es valido para sistemas que no hagan un log de los logins y que no tienen un limite maximo de intentos. La lista puede ser un poco mas larga, pero no mucho, porque este sistema es tambien lento.
-O con un crackeador de ficheros de password, esto solo vale si tienes acceso al fichero de passwords. Este metodo es el mas rapido y se puede usar una lista larga (si dispones de tiempo).

$Tipos de passwords -->
-Genericos, son claves tipicas, muy usadas y que son posibles de encontrar en cualquier ordenador, como guest, root, etc...
-Particulares, solo sirven para una determinada cuenta o ordenador, son datos relacionados con el poseedor de la cuenta.
-Mixtos, son passwords genericos en algunos casos, como son passwords en espa¤ol (solo sirven para ordenadores de habla hispana) los passwords por defecto de los distintos sistemas operativos (solo sirven en ordenadores que usen ese sistema. Mirar articulo, sobre passwords por defecto) y todos aquellos que afecten a un grupo determinado de ordenadores.

?Es una clasificacion un poco de andar por casa, la he puesto para orientar un poco a la hora de describir como hacer una lista de ataque.

$Que contiene --> Voy a dar un guion de lo que una lista de ataque debe contener, siguiendo un orden de importancia decreciente:
-Datos del poseedor de la cuenta, como son nombre, apellido, alias, etc...
-Datos relacionados con el, el nombre de su mujer, de su perro, cosas relacionadas con su trabajo.
-Aficiones y palabras relacionadas con el poseedor de la cuenta o del sysop, como musica, actores, juegos...
-Palabras relacionadas con el ordenador a hackear, como son, el lugar donde se encuentra, su nombre, etc...
-Datos relacionados con el administrador del sistema, ya que algunas veces es el que se encarga de asignar los passwords.
-Una lista de la mayoria de los nombre de persona, y si puede ser motes, iniciales, apodos y apellidos.
-Palabras relacionadas con la informatica.
-Claves tipicas, como abrete sesamo, hola, dios...
-Claves numericas tipicas, como 111111, 123456, etc...
-Cosas cercanas al ordenador, como mesa, lapiz, etcetera.
-Palabras que aparezcan el la pantalla, login, wellcome, y demas.
-Siglas.

?No os tomeis este orden al pie de la letra, segun la informacion que tengais del ordenador a hackear, podeis variar el orden y centraros en apectos mas concretos si teneis mucha informacion, o en aspectos mas genericos, si desconoceis la identidad del posedor, etc... Sobre todo pensarlo mucho

y echarle mucha imaginacion.

$Como hacerla --> Bueno, con todos los datos que te he dado, mas o menos sabras como hacer tu propia lista de passwords, ademas si necesitas un poco de ayuda, puedes encontrar una lista de ejemplo en el numero dos de esta misma publicacion.

Con un poco de imaginacion y despues de investigar bien tu objetivo podras empezar a hacer tu lista, no te preocupes, si no te sale la primera vez. Primero haz un boceto de lo que tu lista va a contener y despues ve a¤adiendo palabras a cada apartado, y luego repasalo y borra los que parezcan muy malos y a¤ade otros nuevos, hasta que consigas un tama¤o optimo para tu objetivo. Entonces solo te queda probarla, si funciona, enhorabuena, si no, vuelve a intentarlo.

eljaker

EOF

3. Lista de passwords por defecto

Esta es la lista de passwords por defecto, de los sistemas operativos mas extendidos. Es un poco antigua, por lo cual, en sistemas recientes no es muy util. Si alguien dispone de alguna un poco mas actualizada, que la envie y la publicaremos.

Mientras tanto, a ver si podeis arreglaros con esta, elaborada partiendo de los datos sacados del "alt.2600 faq" y de "A beginers guide to hacking"

AIX

guest	guest

AS/400

qsecofr	qsecofr
qsysopr	qsysopr
qpgmr	qpgmr
ibm	password
ibm	2222
ibm	service
qsecofr	1111111
qsecofr	2222222
qsvr	qsvr
secofr	secofr

DECserver

ACCESS
SYSTEM

Hewlett Packard MPE-XL

HELLO	MANAGER.SYS	
HELLO	MGR.SYS	
HELLO	FIELD.SUPPORT	HPUNSUP or SUPPORT or HP
HELLO	OP.OPERATOR	
MGR	CAROLIAN	
MGR	CCC	
MGR	CNAS	
MGR	CONV	
MGR	COGNOS	
OPERATOR	COGNOS	
MANAGER	COGNOS	
OPERATOR	DISC	
MGR	HPDESK	
MGR	HPWORD	
FIELD	HPWORD	
MGR	HPOFFICE	
SPOOLMAN	HPOFFICE	
ADVMAIL	HPOFFICE	
MAIL	HPOFFICE	
WP	HPOFFICE	
MANAGER	HPOFFICE	
MGR	HPONLY	

```
FIELD           HPP187
MGR             HPP187
MGR             HPP189
MGR             HPP196
MGR             INTX3
MGR             ITF3000
MANAGER         ITF3000
MAIL            MAIL
MGR             NETBASE
MGR             REGO
MGR             RJE
MGR             ROBELLE
MANAGER         SECURITY
MGR             SECURITY
FIELD           SERVICE
MANAGER         SYS
MGR             SYS
PCUSER          SYS
RSBCMON         SYS
OPERATOR        SYS
OPERATOR        SYSTEM
FIELD           SUPPORT
OPERATOR        SUPPORT
MANAGER         TCH
MAIL            TELESUP
MANAGER         TELESUP
MGR             TELESUP
SYS             TELESUP
MGE             VESOFT
MGE             VESOFT
MGR             WORD
MGR             XLSERVER

Common jobs are Pub, Sys, Data
Common passwords are HPOnly, TeleSup, HP, MPE, Manager, MGR, Remote


Major BBS
~~~~~~~~~
Sysop           Sysop


PICK O/S
~~~~~~~~
DSA
DS
DESQUETOP
PHANTOM


Prolog
~~~~~~
PBX             PBX
NETWORK         NETWORK
NETOP           <null>


Rolm
~~~~
CBX Defaults

op              op
```

```
op              operator
su              super
admin           pwp
eng             engineer


PhoneMail Defaults
~~~~~~~~~~~~~~~~~~
sysadmin        sysadmin
tech            tech
poll            tech


RSX
~~~
SYSTEM/SYSTEM   (Username SYSTEM, Password SYSTEM)
1,1/system      (Directory [1,1] Password SYSTEM)
BATCH/BATCH
SYSTEM/MANAGER
USER/USER
MICRO/RSX

System 75
~~~~~~~~~
bcim            bcimpw
bciim           bciimpw
bcms            bcmspw, bcms
bcnas           bcnspw
blue            bluepw
browse          looker, browsepw
craft           crftpw, craftpw, crack
cust            custpw
enquiry         enquirypw
field           support
inads           indspw, inadspw, inads
init            initpw
kraft           kraftpw
locate          locatepw
maint           maintpw, rwmaint
nms             nmspw
rcust           rcustpw
support         supportpw
tech            field


Taco Bell
~~~~~~~~~
rgm             rollout
tacobell        <null>


Verifone Junior 2.05
~~~~~~~~~~~~~~~~~~~~
Default password: 166816


VMS
~~~
field           service
systest         utep
```

```
UNIX
~~~~
root            root
root            system
sys             sys
sys             system
daemon          daemon
uucp            uucp
tty             tty
test            test
unix            unix
unix            test
bin             bin
adm             adm
adm             admin
admin           adm
admin           admin
sysman          sysman
sysman          sys
sysman          system
sysadmin        sysadmin
sysadmin        sys
sysadmin        system
sysadmin        admin
sysadmin        adm
who             who
learn           learn
uuhost          uuhost
guest           guest
host            host
nuucp           nuucp
rje             rje
games           games
games           player
sysop           sysop
root            sysop
demo            demo


PRIME
~~~~~
PRIME           PRIME
PRIME           PRIMOS
PRIMOS          PRIMOS
PRIMOS          PRIME
PRIMOS_CS       PRIME
PRIMOS_CS       PRIMOS
PRIMENET        PRIMENET
SYSTEM          SYSTEM
SYSTEM          PRIME
SYSTEM          PRIMOS
NETLINK         NETLINK
TEST            TEST
GUEST           GUEST
GUEST1          GUEST


DEC10
~~~~~
1,2:        SYSLIB or OPERATOR or MANAGER
2,7:        MAINTAIN
5,30:       GAMES
```

IRIS
~~~~
MANAGER
BOSS
SOFTWARE
DEMO
PDP8
PDP11
ACCOUNTING

Como casi siempre pasara, estos passwords, no funcionaran en ningun ordenador, pero no os preocupeis, por algo hay que empezar y a lo mejor si el administrador es muy torpe, puede que se haya dejado alguna cuenta de root, a la vista.

eljaker

*EOF*
~~~~

4. Escaneo de lineas en ESPA¥A

A) Breve introduccion (para novatos) - Bueno, para los nuevos en esto, voy a explicar mas o menos en que consiste el escaneo de lineas (telefonicas)

Pues escanear lineas consiste en llamar (por telefono) a varios numeros, siguiendo un orden. Esto sirve para localizar "carriers", es decir, modems conectados al telefono. ¨Y para que sirve esto? Pues macho, para lo de siempre, para hackearlos.

Para ello se usan programas que llaman automaticamente a los numeros que les indiques. Estos programas se llaman war-dialers, daemon-dialers, discadores, etc... La palabra war-dialer es la mas usada y viene de la pelicula juegos de guerra (war-games-dialer) en la que se podia ver como el protagonista hacia un escaneo de lineas y acaba encontrando el ordenador "gordo".

O sea, tu al programa le dices que llame desde el numero 1234000 hasta el 1234999, es decir, escanear unos 1000 numeros, cosa que seria imposible realizar a mano. Los war-dialers, suelen ser lentos, ya que esperan un n§ de tonos hasta llamar al siguiente, pero hay algunos trucos para que lo hagan mas rapido.

hay varios war-dialers en el mercado, no os puedo recomendar ninguno en especial, pero incluso hay uno en espa¤ol (lo podeis encontrar en iberhack=http://www.geocities.com/SiliconValley/park/7574/) Tambien podeis haceros uno vosotros mismos, es bastante facil, e incluso lo podeis hacer mediante los scripts que llevan algunos programas de comunicaciones como el telix.

B) ESPA¥A, condiciones generales - La verdad es que el escaneo de lineas en espa¤a es bastante dificil, mucho mas que en USA, y es que la telefonica espa¤ola es bastante dura con los "nuestros". En paises como USA o UK hay listas enormes de carriers, localizados mediante esta tecnica, pero es Espa¤a se ha hecho muy pocas veces, y solo hay unos pocas listas (como "las paginas rojas") con pocos numeros, y solo de ciudades como Madrid y Barcelona o de numeros 900 (AVISO; ni se os ocurra hackear, ni escanear, en telefonos 900, porque localizan automaticamente al llamante, y os puede caer un puro. Ya hablaremos de esto en proximos numeros)

Ademas con las caracteristicas de la telefonia espa¤ola, es muy facil, localizar llamadas, incluso de moviles, con lo que usar el telefono de casa es casi un suicidio. Por eso hay van unos consejos.

C) Tecnicas para un escaneo seguro:

-Si es posible utiliza un telefono "limpio", es decir, que no tenga relacion contigo y en el que no te puedan pillar, como seria, el telefono de un vecino un primo, o si tienes un portatil, en una de las nuevas cabinas, con clavija para modem.

-Tambien es aconsejable usar un movil, ya que es mas dificil de localizar.

-Escanea a altas horas de la madrugada o si no puedes, en horarios de mucho uso de las lineas. Llamar muy de noche, es muy ventajoso, ya que a esas horas nadie cojera el telefono, ahorrandonos unas pelas y hacelerando el escaneo. Si no puedes estar levantado hasta esas horas, tambien puedes escanear en horas de mucho uso telefonico, ya que a estas horas sera mas dificil que te localicen.

-Configura el war-dialer, para que cuelgue muy pronto, es decir, con 3 o 4 pitidos hay mas que suficiente, ya que la mayoria de modems cojen la llamada tras la primera se¤al. De esta manera, ahorraremos tiempo, conseguiremos que la gente no llegue a tiempo de coger los telefonos de voz, y ahorraemos unas pelillas. Incluso, puedes reducir el numero de tonos, a 2 o incluso 1 si llamas a horas poco aptas.

-Con el truco anterior o llamando a horas raras, conseguiras que no descuelguen telefonos de voz, esto ademas de hacerte ahorrar dinero tiene 2 ventajas, en la factura no saldran los 100 numeros que has escaneado, ya

que si el otro lado no descuelga, la llamada no se contabiliza, esto a su vez es la segunda gran ventaja, si la otra parte no descuelga, no quedan practicamente registros de tu llamada, con lo cual sera mas dificil que te localicen.
-Procura configurar el war-dialer, para que no llame en orden lineal (es decir, siguiendo un orden claro, ascendente o descendente), ya que los de telefonica te localizarian, haz que llame de una forma que parezca aleatoria, es decir si escaneas desde el X00 al X99 primero que llame al X84 luego al X57 y asi de una forma que parezca casual.
-No escanees mucho tiempo seguido, ni un numero muy grande de telefonos. Si te cogen el telefono mas de 10 o 12 veces, deja de llamar, hasta dentro de un par de dias.
- Deja algunos dias entre cada escaneo, no lo hagas a diario, ni siguiendo una pauta fija.
-Llama los fines de semana o en periodos vacacionales, o cuando haya menos gente atenta al telefono.
-Por supuesto si tienes conocimientos de telefonia, podrias intentar algun truco tecnico, como modificar un telefono GSM, o algo por el estilo, para evitar ser detectado, pero siempre teniendo en cuenta que estos sistemas, suelen ser localizados tarde o temprano, a si que usalos poco.
-Usa las reglas basicas del hacker, no lo comentes con nadie, se discreto, etc...
-Investiga un poco antes de empezar a escanear, mira la guia telefonica y busca zonas interensantes. En Espa¤a no pasa como en USA, donde los distritos telefonicos, corresponden directamente a zonas geograficas o comerciales, pero los telefonos siguen una pauta aproximada, por ejemplo los telefonos del mismo barrio suelen empezar por los mismos numeros, lo mismo se pasa en universidades, ministerios, etc... Por ejemplo si el telefono de la centralita de un instituto, empieza por 123, seguramente el telefono del modem de ese instituto, tambien empezara por 123.
-Tambien seria muy util poseer, una guia telefonica en cd-rom, de esta manera se podria hacer un escaneo-off-line, es decir, comprobar a quien corresponde cada numero de telefono, sin necesidad de llamar.

Hay algunas tecnicas mas, que ahora no se me ocurren. Planealo bien, piensa mucho y consigue buenos contactos, pero sobre todo mucha cautela y mucha suerte...

eljaker

EOF

5. DESPEDIDA:

Aqui se acaba la tercera entrega de esta revista, espero que os haya gustado y que os animeis a colaborar y a mandar material.

la proxima semana, trataremos asuntos aun mas interesantes, y espero que nuestros colaboradores empiecen a trabajar.

hasta entonces.

eljaker

$$ Los otros numeros de esta revista pueden encontrarse en:

- BBS CLUB (Murcia)
968-201819 y 968-201262

- y en internet en (iberhack)
http://www.geocities.com/SiliconValley/park/7574/

$$ Para contactar con nosotros, pasate por el area de hackin-crackin de BBS CLUB o por los canales #warezspain y #iberhack del irc (Undernet y irc.arrakis.es), y pregunta por eljaker.

$$ O en esta direccion: eljaker@hotmail.com

EOF